UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, *on behalf of himself and all others similarly situated*,

Plaintiff,

-against-

ALLY BANK and ALLY FINANCIAL, INC.,

Defendants.

No. 21 Civ. 6799 (NSR)
OPINION & ORDER

NELSON S. ROMÁN, United States District Judge:

This putative class action alleges that Defendants Ally Bank and Ally Financial, Inc. (collectively, "Defendants") recklessly or negligently disseminated their customers' account usernames and passwords to unnamed, unauthorized third parties through a coding error in Defendants' website portal (the "Coding Error") and failed to take reasonable measures to maintain the confidentiality of those usernames and passwords. (Amended Complaint ¶¶ 1–12, ECF No. 45.) Plaintiff David De Medicis, on behalf of himself and all others similarly situated, brings this action against Defendants asserting claims for negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, violations of the Virginia Personal Information Breach Notification Act and the North Carolina Unfair and Deceptive Trade Practices Act, and injunctive/declaratory relief under the Declaratory Judgment Act. (*Id.* ¶¶ 147-206.) Presently before the Court is Defendants' motion to dismiss Plaintiff's Amended Complaint under Federal Rules of Civil Procedure 12(b)(1) and (6). (ECF No. 49.) For the following reasons, the Court GRANTS Defendants' motion to dismiss.

BACKGROUND

I. Factual Background

The following facts are derived from the Amended Complaint ("AC"), and are taken as true and construed in the light most favorable to Plaintiff for the purposes of this motion. The following facts are also derived from Defendants' proffered extrinsic evidence purportedly revealing the existence of factual problems in the assertion of jurisdiction.[1]

Plaintiff, a Virginia resident, maintains checking, savings, and securities accounts with Defendant Ally Bank, a direct banking subsidiary of Defendant Ally Financial, a digital financial-services company. (AC ¶¶ 19–21.) Ally Bank, a virtual bank that receives deposits directly from consumers, required Plaintiff and class members to provide usernames and passwords to open and maintain accounts with Ally Bank. (*Id.* ¶¶ 28, 36.) Ally Bank processed and stored those usernames and passwords on its computer systems. (*Id.* ¶ 36.)

On April 12, 2021, during a routine website update, Defendants learned of the Coding Error, which affected certain query strings that transmit information after a customer entered a username and password to access an online account with Defendants. (Hall Decl. ¶ 4, ECF No. 51.) These query strings—which send information across Defendants' platform to allow customers to access their online accounts—usually do not contain any personally identifiable information. (Hall Decl. ¶¶ 5–6.) The Coding Error, however, resulted in certain query strings that contained usernames and passwords (embedded within the string of code) being sent to a limited group of known entities with which Defendants have ongoing contractual and business relationships. (*Id.*

[1] "A defendant is permitted to make a fact-based Rule 12(b)(1) motion, proffering evidence beyond the Pleading[,] [such as through] . . . affidavits submitted [that] . . . reveal the existence of factual problems in the assertion of jurisdiction." *Carter v. HealthPort Techs.*, LLC, 822 F.3d 47, 57 (2d Cir. 2016) (internal quotation marks and citations omitted).

¶¶ 7-8.) For example, a query string with a customer's username and password (both redacted) looked like this:

> https://www.ally.com,/,/,/?hdmjavascriptdata=&allysf-login-v1-account=aaos&allysf-login-v1-username-78e30d704ccce8ccc7b8539f0144cb09=[redacted]&allysf-login-v1-password-78e30d704ccce8ccc7b8539f0144cb09=[redacted]

(*Id.* ¶ 10.) The Coding Error only occurred in limited circumstances where the user attempted to log in before the page had fully loaded—that is, when the user was using software to automatically populate the username and password. (*Id.* ¶ 7.)

Immediately upon learning of the Coding Error, Defendants updated the affected code to eliminate the error. (*Id.* ¶ 13.) Defendants also implemented a process that required all potentially affected customers—whether or not they were actually affected—to change their password. (*Id.* ¶ 14.) Defendants also began working with the businesses to which the query strings may have been visible to purge the information. (*Id.* ¶ 15.) Defendants represent that all of these entities agreed to delete the information, and all subsequently confirmed deletion. (*Id.*)

Defendants also immediately began investigating which customers' usernames and passwords may have been embedded in the query strings due to the Coding Error. (*Id.* ¶ 17.) Defendants represent that they had to parse through millions of website login attempts and, for each login attempt, identify whether the Coding Error had actually occurred during the login attempt and, if so, match the information to a specific customer. (*Id.*) Defendants represent that they identified each of their customers who could have been potentially impacted by the Coding Error. (*Id.* ¶ 18.)

Defendants also began fraud-monitoring efforts to assess threats or risks of fraud specific to the Coding Error, including monitoring the accounts of potentially affected customers for fraudulent, suspicious, or anomalous activity. (*Id.* ¶ 16.)

On June 11, 2021, Defendants sent a letter to those customers whose information had been embedded in the query strings as a result of the Coding Error. (*Id.* ¶ 19.) This letter explained the circumstances of the Coding Error and the remedial steps that Defendants took after discovering it, including (1) updating the code; (2) requiring customers to reset their passwords; (3) confirming that all third parties would delete the information; and (4) monitoring customers' accounts. (*See* Hall Decl. ¶¶ 18, 20, Ex. A (copy of letter sent to Plaintiff).) By their letter, Defendants also offered all affected customers free credit monitoring and identity theft insurance coverage for two years. (AC ¶ 123; Hall Decl. ¶ 19, Ex. A.)

Defendants further represent that, since discovering the Coding Error on April 12, 2021, their internal cyber risk and fraud teams have monitored the accounts of affected customers for any increase in potential fraudulent or other anomalous activity. (Hall Decl. ¶ 22.) Defendants represent to have identified no instances of account takeovers, identity theft, or similar occurrences attributable to the Coding Error. (*Id.* ¶ 23.) Additionally, Defendants represent that they have not identified any increased rates of potentially fraudulent activity or other anomalous events attributable to the Coding Error. (*Id.*)

Nonetheless, Plaintiff alleges he suffered not only actual harm but also the imminent threat of future harm. Plaintiff claims that as a result of the breach, malicious actors have targeted and attempted to access the accounts of Ally Bank customers, including Plaintiff's Ally Bank and associated online accounts, "causing Plaintiff to suffer financial and other damages." (AC ¶¶ 14-15, 75-92.) Plaintiff further asserts that following the Coding Error, there was a "wave" of increased fraudulent activity on Ally Bank customers' accounts. (*Id.* ¶¶ 98-124.) Finally, Plaintiff alleges the Coding Error has "compelled [him] to devote many hours of time to ascertain, mitigate and remediate" the effects of the Coding Error, which includes time spent verifying the legitimacy

of Defendants' letter, exploring credit monitoring and identify theft protection, self-monitoring his accounts, addressing unauthorized login attempts, and regaining access to the accounts that he loss access to following the Coding Error. (*Id.* ¶¶ 93–97.)

II. Procedural Background

On August 13, 2021, Plaintiff filed his operative class action Complaint (Compl., ECF No. 5.) On September 17, 2021, Defendants filed a letter seeking leave to file a motion to dismiss, which the Court subsequently granted and for which it set a briefing schedule. (*See* ECF Nos. 10 & 15.) On August 2, 2022, upon review of the parties' respective briefings on Defendants' motion to dismiss, the Court issued an Opinion & Order granting Defendants' motion to dismiss Plaintiff's Complaint, dismissing his claims without prejudice. *De Medicis v. Ally Bank*, No. 21 CIV. 6799 (NSR), 2022 WL 3043669 (S.D.N.Y. Aug. 2, 2022). On December 20, 2022, the Court granted Plaintiff leave to file an Amended Complaint, and he filed the operative Amended Complaint on January 9, 2023.[2] (AC, ECF No. 45.)

On April 20, 2023, with leave of the Court, Defendants filed its papers on the instant motion to dismiss: Motion to Dismiss (ECF No. 49), Memorandum of Law in Support ("Defs. Mem.," ECF No. 50), Declaration of Christian Hall in Support ("Hall Decl.," ECF No. 51), Supplemental Declaration of Christian Hall in Support ("Hall Supp. Decl.," ECF No. 56), Declaration of Rachel Sparks Bradley in Support ("Bradley Decl.," ECF No. 52), and Reply ("Reply," ECF No. 55). That same day, Plaintiff filed his Response in Opposition ("Pl. Opp.," ECF No. 53) and Declaration of David De Medicis in Opposition ("De Medicis Decl.," ECF No. 54).

[2] Plaintiff previously filed an Amended Complaint on October 18, 2022 without leave of the Court. (ECF No. 31.) Pursuant to the parties' Stipulation and Order dated November 9, 2022, Plaintiff withdrew his Amended Complaint dated October 18, 2022 and sought leave of the Court to file the operative Amended Complaint, which the Court granted. (ECF Nos. 40, 44.)

LEGAL STANDARD

I. Federal Rule of Civil Procedure 12(b)(1)

A case is properly dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it. *Makarova v. United States,* 201 F.3d 110, 113 (2d Cir. 2000). The plaintiff bears the burden of establishing the existence of federal jurisdiction. *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560–61 (1992). But "[f]or purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Warth v. Seldin*, 422 U.S. 490, 501 (1975).

"A Rule 12(b)(1) motion challenging subject matter jurisdiction may be either facial or fact-based." *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016). "When the Rule 12(b)(1) motion is facial, *i.e.*, based solely on the allegations of the complaint or the complaint and exhibits attached to it, the plaintiff has no evidentiary burden." *Id.* (citations omitted). "The task of the district court is to determine whether the [complaint and exhibits attached to it] 'allege facts that affirmatively and plausibly suggest that [the plaintiff] has standing to sue." *Id.* (citations omitted). "For purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Warth v. Seldin*, 422 U.S. 490, 501 (1975).

"Alternatively, a defendant is permitted to make a fact-based Rule 12(b)(1) motion, proffering evidence beyond the Pleading." *Carter*, 822 F.3d at 57 (citations omitted). "In opposition to such a motion, the plaintiffs will need to come forward with evidence of their own to controvert that presented by the defendant 'if the affidavits submitted on a 12(b)(1) motion . . . reveal the existence of factual problems' in the assertion of jurisdiction." *Id.* (citing *Exchange National Bank of Chicago v. Touche Ross & Co.*, 544 F.2d 1126, 1131 (2d Cir. 1976)). "However,

the plaintiffs are entitled to rely on the allegations in the Pleading if the evidence proffered by the defendant is immaterial because it does not contradict plausible allegations that are themselves sufficient to show standing." *Id.* "If the extrinsic evidence presented by the defendant is material and controverted, the district court will need to make findings of fact in aid of its decision as to standing." *Id.* Indeed, courts "must" consult factual submissions "if resolution of a proffered factual issue may result in the dismissal of the complaint for want of jurisdiction." *Robinson v. Gov't of Malaysia,* 269 F.3d 133, 140 n. 6 (2d Cir. 2001).

II. Federal Rule of Civil Procedure 12(b)(6)

In deciding a motion to dismiss under Rule 12(b)(6), the Court must accept all factual allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor. *Freidus v. Barclays Bank PLC,* 734 F.3d 132, 137 (2d Cir. 2013). To survive a motion to dismiss, a complaint must contain "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Mere "labels and conclusions" or "formulaic recitation[s] of the elements of a cause of action will not do"; rather, the complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Twombly,* 550 U.S. at 555. In applying these principles, the Court may consider facts alleged in the complaint and documents attached to it or incorporated by reference. *Chambers v. Time Warner, Inc.,* 282 F.3d 147, 152–53 (2d Cir. 2002) (internal quotation marks and citation omitted).

DISCUSSION

In its prior Opinion, the Court dismissed Plaintiff's claims for lack of Article III standing because Plaintiff failed to allege he suffered a concrete, particularized injury-in-fact or a substantial risk of future injury. *De Medicis*, 2022 WL 3043669, at *4–10. In his Amended Complaint, Plaintiff asserts the same claims previously asserted against Defendants for negligence,

negligence *per se*, breach of implied contract, violations of the Virginia Personal Information Breach Notification Act, and injunctive/declaratory relief under the Declaratory Judgment Act, as well as newly added claims for breach of fiduciary duty and violation of the North Carolina Unfair Trade and Deceptive Trade Practices Act. (*See* AC ¶¶ 147-206.) Defendants again seek to dismiss Plaintiff's Amended Complaint for lack of standing—that is, for Plaintiff's failure to allege an injury in fact—and in the alternative, for failure to state a claim. (*See* Defs. Mem. at 9–20.) Specifically, Defendants allege Plaintiff has failed to cure the deficiencies of his Complaint, and that Plaintiff's new allegations neither establish that he suffered an actual injury or that he has a substantial risk of future injury.

As in its prior Opinion, the Court first addresses Defendants' challenge to subject matter jurisdiction and analyzes Defendants' remaining arguments only if the Court has subject matter jurisdiction over the action. *De Medicis*, 2022 WL 3043669, at *4 (citing *Brokamp v. James*, --- F. Supp. 3d ---, No. 1:21-CV-00389 (DNH) (ATB), 2021 WL 5444277, at *2 (N.D.N.Y. Nov. 22, 2021)). For the reasons discussed below, the Court finds Plaintiff fails to plead factual allegations sufficient to establish standing, and thus the Court grants Defendants' motion to dismiss.

I. Standing

Defendants contend that Plaintiff fails to allege either (1) a requisite concrete, particularized, present injury in fact, or (2) a substantial risk of future injury, to sufficiently establish the injury requirement for purposes of Article III standing. (*See* Defs. Mem. at 9–20.)

"Standing is a federal jurisdictional question 'determining the power of the court to entertain the suit.'" *Carver v. City of New York*, 621 F.3d 221, 225 (2d Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 498 (1975)). There are three Article III standing requirements: (1) the plaintiff must have "suffered an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *John v.*

Whole Foods Market Group, Inc., 858 F.3d 732, 736 (2d Cir. 2017) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)). "Each element of standing 'must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation,' and at the pleading stage, 'general factual allegation of injury resulting from the defendant's conduct may suffice.'" *John*, 858 F.3d at 736 (quoting *Lujan*, 504 U.S. at 561).

A. Injury

An injury in fact "'consists of an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.'" *John*, 858 F.3d at 736 (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547–48 (2016)). To satisfy the "injury in fact" element in cases involving allegations of "unauthorized exposure of th[e] plaintiff's data," the complaint must establish either a present injury or a future injury due to the alleged exposure. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 300–01 (2d Cir. 2021). A future injury may satisfy the "injury in fact" requirement "only if the threatened injury is certainly impending, or if there is a substantial risk that the harm will occur." *Id.*

1. Concrete, Particularized Present Injury in Fact

As in their prior motion to dismiss, Defendants argue that Plaintiff's allegations fail to establish he suffered any concrete, particularized present injury in fact. (*See* Defs. Mem. at 10-13.) Plaintiff alleges he suffered the following present injuries: (1) Ally Bank froze Plaintiff's Ally Bank accounts and prohibited Plaintiff from accessing funds in those accounts, which "robbed [] Plaintiff of the opportunity to purchase securities at advantageous market prices" (AC ¶¶ 76-84); (2) Plaintiff experienced multiple unauthorized attempts by malicious actors to access Plaintiff's Ally Bank account, personal email account, and FanDuel account (*id.* ¶¶ 85-92); (3) "[r]epeated targeting of Plaintiff's online accounts has forced Plaintiff to devote substantial time to mitigate and remediate the adverse effects" of the Coding Error (*id.* ¶¶ 93-97); (4) a malicious actor gained

unauthorized access to and made unauthorized transactions on Plaintiff's Coinbase and Amazon accounts (*id.* ¶¶ 109-112, 114-115); and (5) Plaintiff has loss access to funds in his account on several occasions due to fraudulent activity on his account (*id.* ¶¶ 110, 113).

With regards to unauthorized attempts to access Plaintiff's personal email, FanDuel, and Ally Bank accounts and Plaintiff's time spent mitigating and remediating the effects of the Coding Error, the Court has already addressed both of these alleged injuries and declines to rehash its conclusions here. *See De Medicis*, 2022 WL 3043669, at *5, 6-8. As Plaintiff fails to make any new allegations with respect to these alleged harms, the Court adheres to its previous determination. Accordingly, unauthorized attempts on Plaintiff's accounts are insufficient to constitute a particularized, concrete injury, and Plaintiff's "time spent" may only constitute a present injury if he can establish a substantial risk of future injury of identity theft. *Id.* at *5-6.

The Court addresses Plaintiff's remaining allegations of present injury in turn.

a) Loss of Opportunity to Invest

With respect to the first alleged present injury, Plaintiff claims that "Ally's freezing of Plaintiff's accounts [from August 18, 2021 to August 27, 2021] robbed [him] of the opportunity to purchase securities at advantageous market prices such as the Vanguard Russell 1000 Growth ETF." (AC ¶¶ 76, 82.) Construing the allegations in the light most favorable to Plaintiff and accepting as true that he intended to purchase the securities at the more advantageous price while his account was frozen, Plaintiff may have suffered a concrete injury through the loss of the opportunity to invest. *See Rosario v. Icon Burger Acquisition LLC, No. 21-CV-4313(JS)(ST)*, 2022 WL 198503, at *3 (E.D.N.Y. Jan. 21, 2022) ("[A]bsent factual allegations that the plaintiff forewent the opportunity to invest . . . he cannot plausibly claim he suffered a harm sufficiently concrete to establish Article III standing."); *Epstein v. JPMorgan Chase & Co.*, No. 13 CIV. 4744

KPF, 2014 WL 1133567, at *7 n.6 (S.D.N.Y. Mar. 21, 2014) (stating plaintiff could "theoretically" premise standing on his inability to "use and/or earn interest"). However, to establish standing, Plaintiff must still allege that this injury is "fairly traceable to the challenged conduct of the defendant." *Max v. Kaplan*, No. 23-201-CV, 2024 WL 276717, at *1 (2d Cir. Jan. 25, 2024). As the Court previously acknowledged, the freeze on Plaintiff's Ally Bank accounts between August 18, 2021 and August 27, 2021 was due to the litigation hold issued by Defendants and not a result of the Coding Error. *De Medicis*, 2022 WL 3043669, at *4; (Reply at 2; De Medicis Decl. ¶¶ 9-12; Hall Decl. ¶¶ 25-27.) Notably, Plaintiff does not address this argument in his opposition. (*See* Pl. Opp. at 14.) Accordingly, Plaintiff has failed to plead a causal connection between the Coding Error and his loss in investment opportunity.

b) Unauthorized Transactions on Plaintiff's Amazon and Coinbase Accounts

Plaintiff alleges the passwords disseminated during the Coding Error were used to access and make unauthorized purchases on Plaintiff's Coinbase and Amazon accounts. Plaintiff fails, however, to establish a present harm because the supposed financial losses from these transactions were fully refunded. Plaintiff alleges that on or about October 21, 2021, a "malicious actor" broke into Plaintiff's Coinbase account and "spen[t] down the total value of cryptocurrency then on deposit in Plaintiff's Coinbase account" before attempting to "initiate[] a transfer of funds from Plaintiff's bank account at Wells Fargo to purchase $5,000 of Bitcoin in Plaintiff's Coinbase [account]." (AC ¶ 109.) Although Wells Fargo rejected the transfer due to insufficient funds, "Coinbase held Plaintiff liable for the $5,000 purchase." (*Id.*) However, Coinbase eventually refunded Plaintiff the amounts fraudulently drawn with Plaintiff's Coinbase payment card. (*Id.* ¶ 112.) On or about October 28, 2022, fraudsters also hacked Plaintiff's Amazon account and "attempted purchases using the Plaintiff's credit cards." (*Id.* ¶ 114.) While the fraudsters

successfully made two unauthorized purchases on Plaintiff's Amazon account, "Amazon subsequently refunded [] Plaintiff's account for those two fraudulent purchases." (*Id.* ¶ 115.)

Again, Plaintiff fails to address the refunding of money loss due to unauthorized transactions, instead focusing his argument on "malicious actors" continuing to have the ability to cause actual, as opposed to theoretical, financial losses. The Court will address this argument below when determining whether Plaintiff has alleged a substantial risk of future harm. With respect to Plaintiff's allegations of present harm, these alleged injuries are insufficient. As Plaintiff concedes, he was fully reimbursed for financial losses and therefore has not suffered actual harm. *See Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, *8 (S.D.N.Y. June 25, 2010) (named plaintiffs failed to establish standing because while "their personal information was improperly used," they "acknowledged they were reimbursed for unauthorized charges.") (citing *People to End Homelessness, Inc. v. Develco Singles Apts. Assocs.*, 339 F.3d 1, 9 (1st Cir. 2003)); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016) ("Plaintiff has not alleged that the two fraudulent charges went unreimbursed by his credit union and has experienced no additional actual harm since then."); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 696 (7th Cir. 2015) (reimbursed fraudulent charges may fail to satisfy redressability requirement for standing).

c) Loss of Access to Plaintiff's Accounts Due to Fraudulent Activity

Finally, Plaintiff alleges he suffered harm by temporarily losing access to his accounts in August 2021 and October 2022. (AC ¶¶ 76, 110.) Again, Plaintiff fails to address Defendants' arguments challenging these allegations in his Opposition. Regardless, as Defendants observe, "absent an allegation of how an account freeze resulted in a loss to [Plaintiff], the claim that [he] was injured by the temporary inability to access [his] account does not demonstrate injury."

Rudolph v. Hudson's Bay Co., No. 18-CV-8472 (PKC), 2019 WL 2023713, at *8 (S.D.N.Y. May 7, 2019)

In sum, the Court concludes that Plaintiff fails to cure the deficiencies in his Amended Complaint and his allegations are insufficient to establish that he suffered a concrete, particularized present injury in fact.

2. Substantial Risk of Future Injury

Defendants raise the same arguments in asserting that Plaintiff fails to plead a substantial risk of future injury: (i) the Coding Error was inadvertent and not the result of a targeted attack; (ii) the transmitted information has not been misused; and (iii) the transmitted information was neither sensitive nor high risk. (*See* Defs. Mem. at 13–17.) In its Opposition, however, Plaintiff claims "[t]he landscape has changed tremendously since the filing of the initial complaint" as the effects of the Coding Error "has spread like a mushroom cloud after an explosion." (Pl. Opp. at 13.)

The Court again analyzes Plaintiff's allegations using the *McMorris* factors. In *McMorris v. Carlos Lopez & Associates*, LLC, 995 F.3d 295 (2d Cir. 2021), the Second Circuit held that Article III standing in an "unauthorized data disclosure" action could be based on a "substantial risk of future identity theft or fraud." *Id.* at 300, 303 ("[A] future injury constitutes an Article III injury in fact only 'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'") (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)). From its own and other circuits' precedent, the court drew three factors that "bear on whether the risk of identity theft or fraud is sufficiently 'concrete, particularized, and . . . imminent'" for purposes of Article III standing in data-exposure cases: whether (1) "the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data"; (2) "any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or

fraud"; and (3) "the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *Id.* at 303.

Regarding the first factor, Plaintiff fails to rebut the factual evidence provided by Defendants that the Coding Error was due to an inadvertent programming error and not any targeted attempt. (Hall Decl. ¶ 2; Hall Suppl. Decl. ¶¶ 3-4.) While Plaintiff speculates for the first time in its Opposition that "malicious conduct" may have been the cause,[3] Plaintiff offers no evidence beyond this purely speculative statement. (Pl. Opp. at 4, 8.) Accordingly, as the Court previously determined, this *McMorris* factor weighs against him. *De Medicis*, 2022 WL 3043669, at *9; *see also Carter*, 822 F.3d at 57 (in opposing a fact-based 12(b)(1) motion, plaintiffs must present evidence to rebut evidence by the defendants that reveal the existence of factual problems in the assertion of jurisdiction).

Before reaching the second factor, with regards to the third factor, Plaintiff has failed to raise any new factual allegations so that the Court may reach a different conclusion. As the Court previously recognized and Plaintiff concedes (Pl. Opp. at 16), usernames and passwords are less sensitive information and their dissemination do not pose a high risk of future identify theft or fraud. *De Medicis*, 2022 WL 3043669, at *9. And Plaintiff's assertion that the account usernames and passwords allowed hackers to "get a running jump on exploiting the data" (Pl. Opp. at 16) is also unpersuasive. *In re Practicefirst Data Breach Litig.*, No. 121CV00790JLSMJR, 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022), *report and recommendation adopted*, No.

[3] As this theory was first raised in its Opposition papers, the Court need not even consider it. *See Southwick Clothing LLC v. GFT (USA) Corp.*, No. 99-CV-10452(GBD), 2004 WL 2914093, at *6 (S.D.N.Y. Dec. 15, 2004) ("A complaint cannot be amended merely by raising new facts and theories in Plaintiff's opposition papers, and hence such new allegations and claims should not be considered"); *Tomlins v. Vill. of Wappinger Falls Zoning Bd. of Appeals*, 812 F. Supp. 2d 357, 363 n.9 (S.D.N.Y. 2011) (declining to consider newly raised facts mentioned for the first time in opposition papers); *Feldman v. Sanders Legal Grp.*, 914 F. Supp. 2d 595, 600 n.5 (S.D.N.Y. 2012) (declining to consider arguments in plaintiff's opposition that were "based on facts and theories that are not in the Complaint.").

21CV790JLSMJR, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022) ("[G]eneral allegations in the complaint that individuals whose confidential information has been exposed during a data breach are more likely to experience identity theft in the future are insufficient and conclusory, and do not raise plaintiffs' claim that they are at imminent risk of future harm above a speculative level.").

Finally, with regards to second factor Plaintiff does offer new factual allegations for the Court's consideration. Plaintiff's Amended Complaint includes extensive allegations that the Coding Error resulted in "an explosion of account intrusions, hacked accounts, stolen funds and attempts to steal funds." (Pl. Opp. at 14.) Specifically, Plaintiff alleges (1) fraudsters targeted customers' Ally Bank and associated accounts (*id.* ¶ 14); and (2) in August 2022, there was a "wave of thousands" of unauthorized transactions on Ally Bank customers' debit and credit cards which "demonstrate a misuse of improperly procured data" from the Coding Error (*id.* ¶¶ 98, 10).[4] In support, Plaintiff points to a small business receiving nearly 11,000 small online payments of $1 primarily from Ally Bank card holders—which Plaintiff asserts is a tactic fraudsters use to test whether a stolen credit and debit cards are valid before making more expensive transactions—and a spike in Ally Bank customers posting on the social media website Reddit.com about increased fraudulent activity on their Ally Bank accounts. (*Id.* ¶¶ 99-103, 105-106). Neither of these allegations are sufficient to establish misuse.

[4] Plaintiff also asserts that "[n]ot only were unencrypted Sign-In credentials disseminated to unauthorized recipients, but those unauthorized recipients copied and stored the breached Sign-In Credentials onto their own computer systems" before further disseminating those Sign in Credentials. (AC ¶¶ 49-50.) The Court construes this allegation as referring to Defendants assertion that third-party entities which had contractual and business relationships with Defendants could have had access to the query strings containing usernames and passwords, and those third parties with a direct relationship with Defendants may engage with another party, who thus were engaged in an indirect relationship with Defendants. (Hall Decl. ¶¶ 11-12.) Defendants further assert that third parties with indirect and direct relationships with Defendants confirmed that any disseminated data had been deleted and none of those entities further distributed the data. (Hall Supp. Decl. ¶¶ 4-5.) Plaintiff again does not introduce any evidence rebutting this claim.

Defendants offer evidence that Plaintiff has wrongly attributed the cause of the "wave" of unauthorized transactions to the Coding Error. Rather than a result of inadvertent disclosure of passwords and usernames, the August 2022 spike in fraudulent credit and debit card activity for Ally Bank customers was caused by "BIN attacks, where third parties run scripts on e-commerce sites in order to identify potential card numbers and confirm valid accounts by attempting small transactions." (Hall Supp. Decl. ¶ 7.) Moreover, Defendants identified "no substantial overlap" between customers affected by the Coding Error and customers affected by the 2022 BIN attack. (*Id.*) Again, Plaintiff fails to offer any evidence rebutting these factual assertions.

With regards to the "targeted attacks" on Ally Bank customers on April 19, 2021, May 3, 2021, August 11, 2021, and October 19, 2021, these allegations also fail to hold up under scrutiny. Defendants offer evidence that these targeted attacks were not due to the Coding Error, stating that "[Defendants] have not identified any increased rates of potentially fraudulent activity or other anomalous events attributable to the Coding Error in the accounts of customers affected by the Coding Error." (Hall Supp. Decl. ¶ 6.) At best, Plaintiff alleges an implied temporal connection between the Coding Error and the customer complaints of fraudulent activity. As the Court noted in its prior Opinion, "allegations of only time and space are often insufficient to establish causation." *De Medicis*, 2022 WL 3043669, at *7.

Here, Plaintiff's allegations do not go beyond the temporal—because these are anonymous complaints posted on a public forum it is unclear whether these customers reporting fraudulent activity (1) were even impacted by the Coding Error or (2) had ever previously suffered such incidents of identity theft. *See Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664, 667 (9th Cir. 2007). Both facts are critical to assessing whether the fraudulent activity was plausibly caused by the Coding Error. In fact, the sole argument Plaintiff puts forth regarding these

incidents in his Complaint is that they "were all well within the time period cited by this Court as viable for traceability." (Pl. Opp. at 13-14.) Relying entirely on this temporal connection, Plaintiff's assertions that these anonymous complaints prove a "targeted attack" on Ally Bank customers because of the Coding Error are less than tenuous.[5]

Plaintiff also fails to address many of Defendants' arguments in their motion, which the Court finds persuasive. In particular, Defendants mandated a password request for all potentially impacted customers on April 12, 2021, so any misuse of customers' passwords or usernames after that date, when the credentials were "rendered useless," could not have been plausibly caused by Coding Error. (Defs. Mem. at 14.) That is, of course, unless Ally Bank customers used the same passwords across several accounts. Thus, in alleging that he used the same compromised password for his Coinbase and Amazon accounts, which did thereafter experience unauthorized access and transactions, Plaintiff's argument finally lands on firmer footing. *C.f. Cooper v. Bonobos*, 2022 WL 170622 (finding the second *McMorris* factor against plaintiff where plaintiff does not allege that he used the comprised password on other websites at the time the data breach occurred). Plaintiff further alleges that prior to the Coding Error, his Coinbase account that used the same compromised password had never been hacked. (AC ¶ 111.) Construing Plaintiff's allegations in the light most favorable to him, the Court finds this sufficient to allege misuse. However, the time between the Coding Error and these unauthorized transactions in October 2022 over a year and a half later cuts in Defendants' favor.

Taken together, as in its Complaint, Plaintiff fails to sufficiently allege how the "wave of transactions" or the "targeted attacks" are causally connected to the Coding Error. Moreover,

[5] In examining the alleged incidents more closely, the Court was unable to review the May 3, 2021 incident. The April 19, 2021 alleged incident involved a fraudulent point-of-sale purchase where someone "used [his or her] debit card," and there are no allegations this point-of-sale purchase was related to the anonymous poster's Ally Bank account username and password. (Bradley Decl., Ex. A.)

although Plaintiff properly alleges misuse of his passwords, given the time lapse between the Coding Error and the unauthorized transactions on his Coinbase and Amazon accounts, as well as the other two factors weighing against him, this alleged "misuse" does not carry enough weight to tip the scales completely in his factor.

Weighing the *McMorris* factors, Plaintiff fails to sufficiently allege a substantial risk of future harm. Most significantly, rather than an intentional hack or cyberattack by malicious actors, the Coding Error was an inadvertent dissemination of unencrypted usernames and passwords to entities with which Defendants had business and contractual relationships. *McMorris*, 995 F.3d at 301 ("Where plaintiffs fail to present evidence or make any allegations that an unauthorized third party purposefully obtained the plaintiffs' data, courts have regularly held that the risk of future identify theft is too speculative to support Article III standing."). Upon learning of the breach, Defendants told those entities to delete the inadvertently distributed data and required potentially affected customers to change their passwords. While Plaintiff alleges that his compromised password was used by unauthorized individuals to access his other accounts over a year and a half later, Defendants have not otherwise identified any increase in fraudulent activity or anomalous incidents attributable to the Coding Error. Accordingly, Plaintiff's Amended Complaint relies on the sort of "attenuated chain of possibilities" rejected by the Supreme Court: the Court would have to assume that the entities noticed the embedded usernames and passwords, parsed the data from the query strings, and then misused the data themselves or exposed it to a malicious third party, and if the latter, the third party misused the comprised passwords and usernames after possessing them for months. *See McMorris*, 995 F.3d at 303–304. These allegations are too speculative to confer standing.

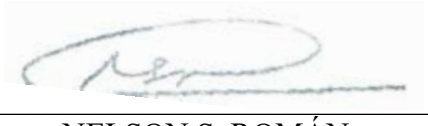
Therefore, the Court concludes that Plaintiff fails to establish the injury requirement for Article III standing and dismiss the Amended Complaint accordingly.

CONCLUSION

For the foregoing reasons, the Court GRANTS Defendants' motion to dismiss (ECF No. 45) and DISMISSES Plaintiff's Amended Complaint with prejudice. The Clerk of the Court is directed to terminate the motion at ECF No. 49 and this action.

Dated: March 25, 2024
White Plains, New York

SO ORDERED:



NELSON S. ROMÁN
United States District Judge